

COMPUTER SECURITY PROBLEM AREAS *

A. STORAGE PROBLEMS

1. Mass storage problem with vulnerability of volume of data in small area.
2. Storage media handling problems:
 - a. Magnetic tapes.
 - b. Discs.
 - c. Drums.
 - d. Data cell.

B. OPERATIONAL TYPE PROBLEMS

1. Electro-magnetic radiation.
2. Wiretapping.
3. Spillage and penetration in multi-level system:
 - a. Accidental spillage.
 - b. Planned penetration.

C. ADJUNCTIVE PROBLEMS

1. Degaussing of storage media.
2. Remote terminal vulnerability.
3. Security classification and dissemination controls.

*Digest of problems as outlined by
Office of Security, CIA, in "A Presentation on Security in the
Automatic Data Processing Environment", attachment to
IBSEC-M-104, 16 April 1968.

25X1

Possible Computer Security Problem Areas - NSA

1. Protection of the information or files of the Computer System

Since files may contain information of different levels of sensitivity and/or classification, the access to these files by users must be rigidly controlled.

2. Clearance of Operating Personnel - required level and need-to-know

The problem of controlling need-to-know in multi-level/multi-access computer systems becomes more complex.

3. Identification of User

Assurance must be made that only those users authorized to have access will receive the desired information. In addition to clearance determination, such things as code names, compartmented name, handling caveats, etc. must be given consideration to insure proper need-to-know.

4. Classification of information derived from multi-sources.

5. Protection of communication links and equipment from emanation and possibly direct line taps.

6. Providing adequate physical security safeguards in storage and computer areas.

7. Insuring that proper safeguards are maintained to prevent override or cross talk within the hardware of the system.

SECURITY PROBLEM AREAS - FBI

1. Sanitization of storage media, primarily discs.
2. Security of computer data transmissions over leased and/or switched common carrier communications lines.
 - a. Terminal security with "need to know" procedures.
 - b. Protection against electronic interception.
 - c. Encryption devices.
3. Security of areas of core containing classified data in a multiprogramming environment.
4. Establishment and maintenance procedures for secure tape and disc library.